3

Security Options Comparison

Windows Server 2003 provides a number of Security Options that can be applied within the scope of managing a GPO. Most are the same as those available in Windows 2000. However, in Windows Server 2003, many names have changed, and some options have been expanded as separate settings to give you more control. Table 3.1 shows how Windows 2000 Security Options map to Windows Server 2003 Security Options. This table does not list all the new options, but rather just maps the options between Windows 2000 and Windows Server 2003.

To find the complete list of options, open the Group Policy Object Editor and browse to Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Security Options.

Tables 3.1 and 3.2 contain the same information. However, the items in Table 3.1 are alphabetized by the name of the Windows 2000 Security Option, and the items in Table 3.2 are alphabetized by the name of the Windows Server 2003 Security Option.

TABLE 3.1 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows 2000 Security Options

Windows 2000 Security Options	Windows Server 2003 Security Options
Additional restrictions for anonymous connections	Network access: Do not allow anonymous enumeration of SAM accounts
Allow server operators to schedule tasks (Domain Controllers only)	Domain Controller: Allow server operators to schedule tasks
Allow system to be shut down without having to log on	Shutdown: Allow system to be shut down without having to log on
Allowed to eject removable NTFS media	Devices: Allowed to format and eject removable media
Amount of idle time required before disconnecting session	Microsoft network server: Amount of idle time required before suspending session

TABLE 3.1 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows 2000 Security Options *(continued)*

Windows 2000 Security Options	Windows Server 2003 Security Options
Audit the access of global system objects	Audit: Audit the access of global system objects
Audit the use of Backup and Restore privilege	Audit: Audit the use of Backup and Restore privilege
Automatically log off users when logon time expires	Network security: Force logoff when logon hours expire
Automatically log off users when logon time expires (local)	Microsoft network server: Disconnect clients when logon hours expire
Clear virtual memory pagefile when system shuts down	Shutdown: Clear virtual memory pagefile
Digitally sign client communication (always)	Microsoft network client: Digitally sign communications (always)
Digitally sign client communication (when possible)	Microsoft network client: Digitally sign communications (if server agrees)
Digitally sign server communication (always)	Microsoft network server: Digitally sign communications (always)
Digitally sign server communication (when possible)	Microsoft network server: Digitally sign communications (if client agrees)
Disable Ctrl+Alt+Del requirement for logon	Interactive logon: Do not require Ctrl+Alt+Del
Do not display last user name in logon screen	Interactive logon: Do not display last user name
LAN Manager authentication level	Network security: LAN Manager authentication level
Message text for users attempting to log on	Interactive logon: Message text for users attempting to log on
Message title for users attempting to log on	Interactive logon: Message title for users attempting to log on
Number of previous logons to cache (in case Domain Controller is not available)	Interactive logon: Number of previous logons to cache (in case Domain Controller is not available)

TABLE 3.1 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows 2000 Security Options *(continued)*

Windows 2000 Security Options	Windows Server 2003 Security Options
Prevent system maintenance of computer account password	Domain member: Disable machine account password changes
Prevent users from installing printer drivers	Devices: Prevent users from installing printer drivers
Prompt user to change password before expiration	Interactive logon: Prompt user to change password before expiration
Recovery Console: Allow automatic administrative logon	Recovery Console: Allow automatic administrative logon
Recovery Console: Allow floppy copy and access to all drives and all folders	Recovery Console: Allow floppy copy and access to all drives and all folders
Rename administrator account	Accounts: Rename administrator account
Rename guest account	Accounts: Rename guest account
Restrict CD-ROM access to locally logged-on user only	Devices: Restrict CD-ROM access to locally logged-on user only
Restrict floppy access to locally logged-on user only	Devices: Restrict floppy access to locally logged-on user only
Secure channel: Digitally encrypt or sign secure channel data (always)	Domain member: Digitally encrypt or sign secure channel data (always)
Secure channel: Digitally encrypt secure channel data (when possible)	Domain member: Digitally encrypt secure channel data (when possible)
Secure channel: Digitally sign secure channel data (when possible)	Domain member: Digitally sign secure channel data (when possible)
Secure channel: Require strong (Windows 2000 or later) session key	Domain member: Require strong (Windows 2000 or later) session key
Secure system partition (for RISC platforms only)	N/A
Send unencrypted password to connect to third-party SMB servers	Microsoft network client: Send unencrypted password to third-party SMB servers

TABLE 3.1 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows 2000 Security Options *(continued)*

Windows 2000 Security Options	Windows Server 2003 Security Options
Shut down system immediately if unable to log security audits	Audit: Shut down system immediately if unable to log security audits
Smart card removal behavior	Interactive logon: Smart card removal behavior
Strengthen default permissions of global system objects (for example, Symbolic Links)	System objects: Strengthen default permissions of internal system objects (for example, Symbolic Links)
Unsigned driver installation behavior	Devices: Unsigned driver installation behavior
Unsigned nondriver installation behavior	N/A
N/A	Accounts: Administrator account status (Windows 2003/SP1 only)
N/A	Accounts: Guest account status
N/A	Accounts: Limit account use of blank passwords to console logon only
N/A	DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax (Windows 2003/SP1 only)
N/A	DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax (Windows 2003/SP1 only)
N/A	Devices: Allow undock without having to log on
N/A	Domain Controller: LDAP server signing requirements
N/A	Domain Controller: Refuse machine account password changes
N/A	Domain member: Maximum machine account password age

TABLE 3.2 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows Server 2003 Security Options

Windows Server 2003 Security Options	Windows 2000 Security Options
Accounts: Administrator account status (Windows 2003/SP1 only)	N/A
Accounts: Guest account status	N/A
Accounts: Limit account use of blank passwords to console logon only	N/A
Accounts: Rename administrator account	Rename administrator account
Accounts: Rename guest account	Rename guest account
Audit: Audit the access of global system objects	Audit the access of global system objects
Audit: Audit the use of Backup and Restore privilege	Audit the use of Backup and Restore privilege
Audit: Shut down system immediately if unable to log security audits	Shut down system immediately if unable to log security audits
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax (Windows 2003/SP1 only)	N/A
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax (Windows 2003/SP1 only)	N/A
Devices: Allow undock without having to log on	N/A
Devices: Allowed to format and eject removable media	Allowed to eject removable NTFS media
Devices: Prevent users from installing printer drivers	Prevent users from installing printer drivers
Devices: Restrict CD-ROM access to locally logged-on user only	Restrict CD-ROM access to locally logged-on user only
Devices: Restrict floppy access to locally logged-on user only	Restrict floppy access to locally logged-on user only

TABLE 3.2 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows Server 2003 Security Options *(continued)*

Windows Server 2003 Security Options	Windows 2000 Security Options
Devices: Unsigned driver installation behavior	Unsigned driver installation behavior
Domain Controller: Allow server operators to schedule tasks	Allow server operators to schedule tasks (Domain Controllers only)
Domain Controller: LDAP server signing requirements	N/A
Domain Controller: Refuse machine account password changes	N/A
Domain member: Digitally encrypt or sign secure channel data (always)	Secure channel: Digitally encrypt or sign secure channel data (always)
Domain member: Digitally encrypt secure channel data (when possible)	Secure channel: Digitally encrypt secure channel data (when possible)
Domain member: Digitally sign secure channel data (when possible)	Secure channel: Digitally sign secure channel data (when possible)
Domain member: Disable machine account password changes	Prevent system maintenance of computer account password
Domain member: Maximum machine account password age	N/A
Domain member: Require strong (Windows 2000 or later) session key	Secure channel: Require strong (Windows 2000 or later) session key
Interactive logon: Display user information when the session is locked (Windows 2003/SP1 only)	N/A
Interactive logon: Do not display last user name	Do not display last user name in logon screen
Interactive logon: Do not require Ctrl+Alt+Del	Disable Ctrl+Alt+Del requirement for logon
Interactive logon: Message text for users attempting to log on	Message text for users attempting to log on
Interactive logon: Message title for users attempting to log on	Message title for users attempting to log on

TABLE 3.2 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows Server 2003 Security Options *(continued)*

Windows Server 2003 Security Options	Windows 2000 Security Options
Interactive logon: Number of previous logons to cache (in case Domain Controller is not available)	Number of previous logons to cache (in case Domain Controller is not available)
Interactive logon: Prompt user to change password before expiration	Prompt user to change password before expiration
Interactive logon: Require smart card	N/A
Interactive logon: Smart card removal behavior	Smart card removal behavior
Microsoft network client: Digitally sign communications (always)	Digitally sign client communication (always)
Microsoft network client: Digitally sign communications (if server agrees)	Digitally sign client communication (when possible)
Microsoft network client: Send unencrypted password to third-party SMB servers	Send unencrypted password to connect to third-party SMB servers
Microsoft network server: Amount of idle time required before suspending session	Amount of idle time required before disconnecting session
Microsoft network server: Digitally sign communications (always)	Digitally sign server communication (always)
Microsoft network server: Digitally sign communications (if client agrees)	Digitally sign server communication (when possible)
Microsoft network server: Disconnect clients when logon hours expire	Automatically log off users when logon time expires (local)
N/A	Secure system partition (for RISC platforms only)
N/A	Unsigned nondriver installation behavior
Network access: Allow anonymous SID/name translation	N/A
Network access: Do not allow anonymous enumeration of SAM accounts	Additional restrictions for anonymous connections

TABLE 3.2 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows Server 2003 Security Options *(continued)*

Windows Server 2003 Security Options	Windows 2000 Security Options
Network access: Do not allow anonymous enumeration of SAM accounts and shares	N/A
Network access: Do not allow storage of credentials or .NET Passports for network authentication	N/A
Network access: Let Everyone permissions apply to anonymous users	N/A
Network access: Named pipes that can be accessed anonymously	N/A
Network access: Remotely accessible registry paths	N/A
Network access: Remotely accessible registry paths and subpaths	N/A
Network access: Restrict anonymous access to named pipes and shares	N/A
Network access: Shares that can be accessed anonymously	N/A
Network access: Sharing and security model for local accounts	N/A
Network access: Do not store LAN Manager hash value on next password change	N/A
Network security: Force logoff when logon hours expire	Automatically log off users when logon time expires
Network security: Force logoff when logon hours expire	N/A
Network security: LAN Manager authentication level	LAN Manager authentication level
Network security: LDAP client signing requirements	N/A

TABLE 3.2 Windows 2000 Security Options vs. Windows Server 2003 Security Options, Alphabetized by the Windows Server 2003 Security Options *(continued)*

Windows Server 2003 Security Options	Windows 2000 Security Options
Network security: Minimum session security for NTML SSP-based (including secure RPC) clients	N/A
Network security: Minimum session security for NTLM SSP-based (including secure RPC) servers	N/A
Recovery Console: Allow automatic administrative logon	Recovery Console: Allow automatic administrative logon
Recovery Console: Allow floppy copy and access to all drives and all folders	Recovery Console: Allow floppy copy and access to all drives and all folders
Shutdown: Allow system to be shut down without having to log on	Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile	Clear virtual memory pagefile when system shuts down
System cryptography: Force strong key protection for user keys stored on the computer	N/A
System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing	N/A
System objects: Default owner for objects created by members of the Administrators group	N/A
System objects: Require case insensitivity for non-Windows subsystems	N/A
System objects: Strengthen default permissions of internal system objects (for example, Symbolic Links)	Strengthen default permissions of global system objects (for example, Symbolic Links)
System settings: Optional subsystems	N/A
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	N/A